



GS PERÚ

Software - Security & Services

Empresas

BOLETÍN CIBERSEGURIDAD

Septiembre - 2026



LA EXPLOTACIÓN ACTIVA Y EL ABUSO DE IDENTIDADES CLOUD MARCAN SEPTIEMBRE

Septiembre 2026: vulnerabilidades críticas, phishing orientado a tokens y automatización adversaria elevan la presión sobre entornos empresariales.

Hasta el 26 de septiembre de 2026, el panorama de ciberseguridad estuvo marcado por dos frentes que se retroalimentan: vulnerabilidades críticas explotadas contra servicios expuestos y campañas que ya no buscan únicamente contraseñas, sino sesiones, tokens, métodos MFA e identidades de aplicaciones. La tendencia favorece técnicas que se mezclan con tráfico y herramientas legítimas, reduciendo señales evidentes de intrusión y aumentando la importancia de correlacionar identidad, endpoint, red y actividad cloud.

En malware, las investigaciones del mes muestran cadenas diseñadas para camuflarse dentro de software o servicios reconocibles. Un instalador alterado de Exodus incorporó un RAT modular con acceso remoto y robo de credenciales; REVSTEALER empleó técnicas antianálisis y la blockchain de Polygon para resolver su infraestructura de C2; MovieReaper aprovechó torrents modificados y la blockchain de Solana para localizar infraestructura de C2; y SectopRAT fue localizado dentro de una copia local manipulada de software legítimo, sin evidencia de compromiso del fabricante.

En vulnerabilidades, la atención se concentra en plataformas con alto valor operativo. CVE-2026-75650 en Adobe Commerce, CVE-2026-20212 en Cisco Nexus 9000, CVE-2026-86218 en N-able N-central y CVE-2026-94127 en BIG-IP APM presentan escenarios de ejecución remota o acceso privilegiado. Adobe Commerce, N-able N-central y BIG-IP APM registran explotación activa; Cisco no reportó explotación maliciosa al emitir su aviso. Los sistemas expuestos antes de la corrección requieren, además del parche, revisión de indicadores, integridad y persistencia.

El phishing y los adversarios reflejan un desplazamiento hacia el control de identidades y la automatización posterior al acceso. Knight Office y GhostCode obtienen tokens después de procesos de autenticación aparentemente válidos, mientras que campañas con señuelos de passkeys buscan persistir mediante nuevos métodos MFA. BREEZE COMET, Storm-2570 y Storm-3168 muestran que RMM, cuentas cloud, service principals y herramientas administrativas pueden convertirse en aceleradores del impacto. La prioridad defensiva es combinar MFA resistente al phishing, control de RMM, privilegio mínimo, protección de identidades de workload y recuperación aislada e inmutable.

ÍNDICE



1. MALWARE 04

- 1.1 Instalador alterado de Exodus oculta un RAT modular con robo de credenciales y acceso remoto
- 1.2 REVSTEALER incorpora técnicas antianálisis y utiliza blockchain para mantener su infraestructura de control
- 1.3 MovieReaper aprovecha torrents alterados y la blockchain de Solana para distribuir una cadena modular
- 1.4 SectopRAT se oculta dentro de software legítimo alterado para mantener control remoto y robar información



2. VULNERABILIDADES 12

- 2.1 CVE-2026-75650 permite ejecución remota sin autenticación en Adobe Commerce y ya es explotada activamente
- 2.2 CVE-2026-20212 permite ejecución remota de código con privilegios root en Cisco Nexus 9000
- 2.3 CVE-2026-86218 permite ejecución remota preautenticada en N-able N-central y registra explotación activa
- 2.4 CVE-2026-94127 permite RCE sin autenticación en configuraciones OAuth de BIG-IP APM



3. PHISHING 20

- 3.1 Knight Office roba sesiones de Microsoft 365 mediante AiTM y persiste registrando dispositivos
- 3.2 Campañas con señuelos de passkeys comprometen identidades cloud y amplían el acceso mediante Microsoft Graph
- 3.3 GhostCode abusa del flujo OAuth Device Code para obtener tokens después de una autenticación legítima



4. ADVERSARIOS 26

- 4.1 BREEZE COMET ataca organizaciones financieras de Brasil para manipular sistemas de pago y realizar transferencias fraudulentas
- 4.2 Storm-2570 mantiene el mismo patrón operativo mientras despliega Qilin, DragonForce, Anubis y BERT
- 4.3 Storm-3168 utiliza service principals comprometidos para reconocimiento y destrucción automatizada de recursos Azure



5. INDICADORES DE COMPROMISO 32

- 5.1 Direcciones IP
- 5.2 Dominios
- 5.3 Hashes



6. FUENTES 33

1. MALWARE

ALTA

1.1 [ALTA] Instalador alterado de Exodus oculta un RAT modular con robo de credenciales y acceso remoto



Huntress publicó el 1 de septiembre de 2026 el análisis de una campaña en la que usuarios fueron inducidos a ejecutar archivos JavaScript disfrazados de documentos o actualizaciones.

La cadena descargaba un MSI alterado que instalaba una copia funcional de Exodus Wallet 24.33.4, pero ocultaba su interfaz y cargaba en memoria un RAT modular.

El implante incorpora ejecución remota de comandos, administración de archivos, robo de credenciales y cookies de navegadores, proxy SOCKS y VNC oculto.

La persistencia se establece mediante una tarea programada denominada ExdBackupTool, que vuelve a iniciar el componente cada hora.

La comunicación de control utiliza Azure Table Storage como mecanismo de señalización, reduciendo la dependencia de dominios propios y dificultando la detección basada exclusivamente en reputación de red.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Ejecución del usuario	La víctima ejecuta un archivo JavaScript o una supuesta actualización que inicia la cadena maliciosa.	T1204.002
Intérprete de scripts	El archivo inicial utiliza JavaScript/JScript para abrir el señuelo y descargar el instalador.	T1059.007
Persistencia	Una tarea programada ExdBackupTool relanza el componente de Exodus desde el perfil del usuario.	T1053.005
Acceso a credenciales	El módulo de navegador recupera credenciales, cookies y extensiones almacenadas.	T1555.003
Proxy	El RAT incorpora un módulo SOCKS que permite utilizar el equipo comprometido como relay.	T1090

Recomendaciones

- Software autorizado: instalar aplicaciones de criptomonedas únicamente desde repositorios oficiales o catálogos corporativos validados.
- Control de scripts: restringir la ejecución de archivos .js descargados y revisar procesos wscript.exe o cscript.exe iniciados desde navegadores.
- Monitoreo de persistencia: alertar por tareas programadas que ejecuten binarios desde AppData o perfiles de usuario.
- Protección de credenciales: investigar accesos anómalos a bases de datos de navegadores, cookies y extensiones desde procesos no autorizados.
- Respuesta: ante detección, aislar el endpoint, eliminar la tarea ExdBackupTool y revisar todos los perfiles del equipo por artefactos equivalentes.

ALTA**1.2 [ALTA] REVSTEALER incorpora técnicas antianálisis y utiliza blockchain para mantener su infraestructura de control**

Elastic Security Labs publicó el 2 de septiembre de 2026 una investigación sobre REVSTEALER, una familia de malware diseñada para robar credenciales almacenadas en navegadores, información de billeteras de criptomonedas y cuentas de plataformas de videojuegos.

La amenaza incorpora mecanismos antianálisis para identificar entornos de sandbox y utiliza la blockchain de Polygon para localizar su infraestructura de comando y control (C2), dificultando la interrupción de sus comunicaciones.

Estas capacidades permiten al malware recopilar información sensible y mantener contacto con su infraestructura maliciosa, lo que representa un riesgo para la confidencialidad de los datos y las credenciales de los usuarios.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Acceso a credenciales	Extracción de credenciales almacenadas en navegadores.	T1555.003
Evasión de defensas	Evaluación del entorno para identificar posibles sandboxes.	T1497
Recolección	Obtención de información de navegadores y billeteras de criptomonedas.	T1005
Comando y control	Uso de blockchain para localizar infraestructura C2.	T1102

Recomendaciones

- Protección de credenciales: supervisar accesos no autorizados a las bases de datos de credenciales de los navegadores.
- Detección de malware: mantener las soluciones EDR actualizadas y supervisar comportamientos asociados con el robo de información.
- Monitoreo de red: investigar conexiones inusuales hacia infraestructura blockchain realizadas por procesos desconocidos.
- Respuesta: aislar los equipos comprometidos, revocar las sesiones afectadas y renovar las credenciales potencialmente expuestas.
- Control de aplicaciones: restringir la ejecución de archivos descargados desde fuentes no confiables y aplicar políticas de listas de aplicaciones permitidas.
- Análisis de comportamiento: identificar procesos que realicen consultas inusuales a servicios blockchain, detecten entornos virtualizados o accedan masivamente a información sensible almacenada en los navegadores.

ALTA**1.3 [ALTA] MovieReaper aprovecha torrents alterados y la blockchain de Solana para distribuir una cadena modular**

Kaspersky publicó el 17 de septiembre de 2026 una investigación sobre MovieReaper, un framework modular distribuido mediante torrents manipulados.

El análisis determinó que el actor modificó el repositorio público itorrents.org, utilizado por varios trackers, de modo que estos entregaban archivos torrent maliciosos sin que cada plataforma hubiera sido comprometida individualmente.

Los ejecutables se presentan como películas populares y utilizan nombres extensos e iconos conocidos para ocultar la extensión .exe.

Tras la ejecución, el loader recupera shellcode y una segunda etapa que consulta una cuenta de la blockchain de Solana para obtener, de forma codificada y cifrada, la dirección de un segundo C2.

La cadena incorpora bypass de UAC, persistencia y un módulo final de administración de archivos con capacidades de carga, descarga, manipulación y previsualización de datos.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Ejecución del usuario	El usuario ejecuta un archivo que aparenta ser contenido multimedia descargado mediante torrent.	T1204.002
Ofuscación	El malware cifra cadenas y oculta la extensión ejecutable mediante nombres largos e iconos de aplicaciones.	T1027
Elevación de privilegios	Una etapa posterior aplica técnicas públicas de bypass de UAC.	T1548.002
Resolución de C2	La blockchain de Solana almacena la dirección cifrada utilizada para localizar el siguiente servidor C2.	T1102.001
Transferencia de herramientas	Las etapas descargan shellcode y módulos adicionales desde infraestructura controlada por el actor.	T1105

Recomendaciones

- Software y contenido confiable: impedir descargas de software o multimedia desde repositorios P2P no autorizados en equipos corporativos.
- Control de extensiones: habilitar la visualización de extensiones conocidas y bloquear ejecutables provenientes de carpetas de descargas.
- Monitoreo de C2: alertar por conexiones hacia deadhub[.]org y por acceso anómalo a infraestructura de blockchain desde procesos desconocidos.
- Protección de privilegios: investigar bypass de UAC y binarios ejecutados desde C:\ProgramData\Microsoft\Windows\Telemetry.
- Hunting: buscar los IoC publicados y revisar endpoints que hayan utilizado torrents o ejecutado archivos con nombres de películas recientes.

ALTA

1.4 [ALTA] SectopRAT se oculta dentro de software legítimo alterado para mantener control remoto y robar información



FortiGuard Incident Response publicó el 24 de septiembre de 2026 el análisis de una variante de SectopRAT, también conocida como ArechClient2, encontrada dentro de una copia local alterada de software legítimo de audio digital.

La evidencia no indica que el fabricante haya distribuido una versión comprometida ni que exista un ataque a su cadena de suministro.

Un componente legítimo, ReportDump.exe, es iniciado mediante una tarea programada y carga una DLL modificada que extrae desde pool.db un payload cifrado de SectopRAT. El RAT opera en memoria, utiliza ofuscación y establece comunicaciones cifradas con su C2.

Sus funciones incluyen control de procesos y archivos, captura de pantalla, ejecución remota y robo de credenciales, cookies, datos de autocompletado, tarjetas guardadas y datos de billeteras de criptomonedas.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Ofuscación	El payload y sus componentes utilizan nombres aleatorios, control-flow flattening y datos cifrados.	T1027
Acceso a credenciales	El RAT extrae credenciales, cookies y datos almacenados por múltiples navegadores.	T1555.003
Captura de pantalla	SectopRAT puede obtener imágenes del escritorio del sistema comprometido.	T1113
Canal cifrado	La comunicación con el servidor C2 se realiza mediante un canal cifrado.	T1573
Canal alternativo	El malware mantiene mecanismos de fallback para resolver infraestructura alternativa.	T1008

Recomendaciones

- Control de integridad: validar firma y hash de DLL y ejecutables presentes en directorios de aplicaciones instaladas.
- Rutas anómalas: investigar software legítimo ejecutado desde C:\ProgramData u otras ubicaciones distintas a su instalación esperada.
- Tareas programadas: alertar por tareas que inicien componentes de reporte, crash dump o utilidades desde carpetas no estándar.
- Protección de credenciales: supervisar accesos masivos a perfiles de navegadores, clientes de correo y billeteras desde procesos desconocidos.
- Bloqueo de C2: incorporar 98[.]142[.]252[.]140 a controles de red y realizar hunting de los hashes publicados por Fortinet.

2. VULNERABILIDADES

CRÍTICA

2.1 [CRÍTICA] CVE-2026-75650 permite ejecución remota sin autenticación en Adobe Commerce y ya es explotada activamente



Adobe publicó el 7 de septiembre de 2026 una actualización urgente para CVE-2026-75650, vulnerabilidad crítica en Adobe Commerce y Magento Open Source con capacidad de ejecución arbitraria de código.

Adobe confirmó explotación activa contra comercios y asignó prioridad 1 al boletín APSB26-146. Sansec, que rastrea la campaña como StyleSmuggler, observó los primeros ataques el 4 de septiembre y describió una técnica que inyecta código PHP en el sistema de plantillas mediante propiedades de estilo.

La ejecución puede activarse durante el renderizado de un correo de pago fallido, sin que el destinatario tenga que abrir el mensaje.

La exposición previa al parche requiere no solo actualizar, sino también revisar compromiso y rotar claves, contraseñas, tokens de integración y secretos potencialmente protegidos por las claves de cifrado de Commerce.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Acceso inicial	Solicitudes remotas especialmente manipuladas explotan una aplicación de comercio expuesta sin autenticación.	T1190
Ejecución	La vulnerabilidad permite que código PHP inyectado sea procesado dentro del contexto de la aplicación.	T1059
Web shell	Sansec observó actividad posterior donde otro actor desplegó un web shell PHP en sistemas explotados.	T1505.003
Transferencia	La actividad posterior puede recuperar componentes o implantes adicionales desde infraestructura externa.	T1105

Recomendaciones

- Aplicar la corrección: desplegar inmediatamente el hotfix asociado a APSB26-146 / VULN-39341 en todas las ramas afectadas.
- Rotar secretos: renovar la clave de cifrado de Commerce y las credenciales, tokens y secretos que pudieron quedar expuestos.
- Threat hunting: revisar tiendas expuestas desde el 4 de septiembre buscando procesos anómalos, web shells y cambios en plantillas.
- Monitoreo de correo: investigar picos inesperados de mensajes Payment Transaction Failed Reminder como posible señal de explotación.
- Reducir exposición: limitar el acceso administrativo y endurecer WAF, CDN y controles de aplicación sin reemplazar la instalación del parche.

CRÍTICA**2.2 [CRÍTICA] CVE-2026-20212 permite ejecución remota de código con privilegios root en Cisco Nexus 9000**

Cisco publicó el 2 de septiembre de 2026 un aviso de seguridad sobre CVE-2026-20212, una vulnerabilidad crítica con una puntuación CVSS de 9.8 que afecta a la integración Silicon One de los switches Cisco Nexus 9000.

Esta falla podría permitir que un atacante remoto no autenticado ejecute código con privilegios root en un dispositivo vulnerable, comprometiendo la confidencialidad, integridad y disponibilidad de la infraestructura de red.

Cisco publicó actualizaciones de software y medidas alternativas para reducir la exposición.

Al momento de emitir el aviso, el fabricante no tenía conocimiento de explotación maliciosa ni de divulgaciones públicas de esta vulnerabilidad.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Reconocimiento	El atacante podría identificar dispositivos Cisco Nexus 9000 y comprobar la exposición de los puertos TCP 43210 y 43211.	T1595.001
Acceso inicial	Se aprovecha la vulnerabilidad en la integración Silicon One mediante entradas especialmente manipuladas enviadas al dispositivo afectado.	T1190
Ejecución	La explotación exitosa podría permitir ejecutar código arbitrario con privilegios root en el sistema operativo del switch.	T1203
Evasión de defensas	Tras un eventual compromiso, el atacante podría modificar mecanismos de seguridad o registros para dificultar su detección.	T1562.001

Recomendaciones

- Actualización de software: instalar las versiones corregidas de Cisco NX-OS correspondientes a los dispositivos afectados.
- Control de acceso: restringir la exposición de los switches y permitir conexiones únicamente desde redes autorizadas.
- Monitoreo de seguridad: supervisar registros y detectar comportamientos anómalos en los dispositivos de red.
- Segmentación de red: limitar la comunicación entre segmentos para reducir el impacto de un posible compromiso.
- Verificación de integridad: revisar configuraciones y cambios no autorizados en los switches afectados.

CRÍTICA

2.3 [CRÍTICA] CVE-2026-86218 permite ejecución remota preautenticada en N-able N-central y registra explotación activa



N-able publicó el 6 de septiembre de 2026 el hotfix 2026.3 HF4 para CVE-2026-86218, una vulnerabilidad crítica capaz de permitir ejecución remota antes de la autenticación sobre servidores N-central.

Tres días después, el fabricante confirmó que había observado un número limitado de explotaciones exitosas contra clientes, mientras que el Canadian Centre for Cyber Security señaló que las versiones anteriores a 2026.3.1.14 estaban afectadas y que CISA incorporó la falla al catálogo KEV.

N-able también publicó indicadores operativos para facilitar la revisión, incluyendo tráfico de escaneo procedente del rango 23.234.64.0/18 y la necesidad de auditar cuentas creadas recientemente o con direcciones de correo anómalas.

Las instancias hospedadas por N-able ya habían sido parcheadas; los despliegues on-premises requieren actualización inmediata.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Escaneo activo	N-able observó conexiones desde 23.234.64.0/18 intentando identificar y explotar sistemas vulnerables.	T1595.002
Acceso inicial	La falla permite atacar una instancia N-central expuesta sin autenticarse previamente.	T1190
Ejecución	La explotación puede conducir a ejecución remota de código en el servidor N-central.	T1059

Recomendaciones

- Actualizar N-central: migrar inmediatamente los servidores on-premises a 2026.3 HF4, build 2026.3.1.14 o posterior.
- Revisar logs: buscar conexiones desde 23[.]234[.]64[.]0/18 y solicitudes inusuales previas a la instalación del hotfix.
- Auditar cuentas: investigar usuarios creados recientemente, correos con dominio inválido y sustituciones de caracteres sospechosas.
- Reducir superficie: restringir el acceso a N-central mediante controles de red y limitar su exposición directa a Internet.
- Respuesta: ante indicadores positivos, preservar registros y coordinar investigación del servidor y de los endpoints administrados.

CRÍTICA**2.4 [CRÍTICA] CVE-2026-94127 permite RCE sin autenticación en configuraciones OAuth de BIG-IP APM**

F5 divulgó el 22 de septiembre de 2026 CVE-2026-94127, una vulnerabilidad de desbordamiento de búfer en heap que afecta a BIG-IP Access Policy Manager.

La explotación permite a un atacante remoto no autenticado ejecutar código cuando BIG-IP APM está configurado como OAuth Authorization Server y el mismo servidor virtual utiliza una política de acceso APM junto con un perfil OAuth.

F5 confirmó explotación activa y JPCERT/CC emitió una alerta el 24 de septiembre con orientación para identificar exposición y aplicar los hotfix disponibles.

Las configuraciones que utilizan APM únicamente como cliente OAuth o Resource Server no están afectadas por este escenario específico.

Por el carácter activo de la explotación, los sistemas expuestos antes del parche requieren revisión de registros e integridad, no solo actualización del software.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia Mitre Att&Ck
Acceso inicial	El atacante dirige solicitudes remotas contra un servicio BIG-IP APM vulnerable y expuesto.	T1190
Ejecución	La corrupción de memoria puede conducir a ejecución de código en el contexto del sistema afectado.	T1059

Recomendaciones

- Identificar exposición: confirmar si APM opera como OAuth Authorization Server con access policy y OAuth profile en el mismo virtual server.
- Aplicar hotfix: instalar la corrección específica publicada por F5 para la rama 21.1, 17.5 o 17.1 correspondiente.
- Mitigación temporal: si el parche no puede aplicarse de inmediato, solicitar a F5 la iRule de mitigación indicada por el fabricante.
- Threat hunting: revisar solicitudes anómalas, comandos, procesos y cambios de integridad en appliances que estuvieron expuestos.
- Restringir administración: limitar interfaces y servicios de gestión a redes confiables y mantener segmentación de infraestructura crítica.

3. PHISHING

ALTA

3.1 [ALTA] Knight Office roba sesiones de Microsoft 365 mediante AiTM y persiste registrando dispositivos



Huntress publicó el 2 de septiembre de 2026 el análisis de Knight Office, un kit de phishing Adversary-in-the-Middle observado durante una intrusión contra Microsoft 365.

La campaña inicia con un correo estilo DocuSign y utiliza redirecciones a través de infraestructura legítima y un sitio Joomla comprometido antes de llegar a la página de phishing.

Knight Office captura tokens de sesión después de que la víctima completa el MFA, permitiendo al atacante reutilizar una sesión ya autenticada sin necesitar la contraseña.

En el incidente investigado, el actor registró un host no autorizado en Microsoft Entra ID y vinculó una credencial de Windows Hello for Business.

Huntress relacionó el panel de control con la IP 104.37.188.94 y observó múltiples ataques asociados al mismo kit, lo que refuerza la necesidad de monitorizar actividad posterior al MFA y registros de dispositivos.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Preparación	Los actores utilizan destinos intermedios y recursos comprometidos para ocultar la página final de phishing.	T1608.005
Phishing	El correo incluye un enlace que conduce a la cadena de redirecciones y a la infraestructura AiTM.	T1566.002
Ejecución del usuario	La víctima accede al enlace malicioso presentado como una solicitud de firma.	T1204.001
Persistencia	El atacante registra un dispositivo no autorizado y vincula credenciales a la identidad comprometida.	T1098.005
Robo de tokens	La infraestructura AiTM intercepta tokens de una sesión autenticada para reutilizarlos posteriormente.	T1528

Recomendaciones

- MFA resistente al phishing: priorizar FIDO2, passkeys administradas y autenticación ligada a dispositivo frente a factores interceptables.
- Conditional Access: exigir dispositivos compliant o administrados para aplicaciones sensibles y sesiones de riesgo elevado.
- Monitoreo post-MFA: detectar autenticaciones desde proxies, nuevos dispositivos o ubicaciones inmediatamente después de un MFA válido.
- Revisar dispositivos: auditar registros recientes en Entra ID y credenciales Windows Hello for Business vinculadas a usuarios afectados.
- Respuesta de identidad: revocar sesiones y tokens, eliminar métodos no autorizados y restablecer credenciales cuando se confirme compromiso.

ALTA

3.2 [ALTA] Campañas con señuelos de passkeys comprometen identidades cloud y amplían el acceso mediante Microsoft Graph



Microsoft Security Research informó el 9 de septiembre de 2026 sobre intrusiones cloud activas observadas desde mayo que utilizan llamadas o mensajes que suplantan al soporte de TI para solicitar una supuesta actualización urgente de passkey, MFA o SSO.

La víctima es dirigida a sitios que imitan el inicio de sesión de Microsoft, pero el objetivo real suele ser capturar credenciales y tokens mediante AiTM o abusar del flujo de autenticación por código de dispositivo.

Después del acceso, los actores registran nuevos métodos MFA o dispositivos para persistencia y realizan reconocimiento intensivo mediante Microsoft Graph.

Microsoft observó búsqueda y descarga de información desde SharePoint y OneDrive, recolección de correo mediante APIs REST y actividad consistente con exfiltración automatizada.

El patrón demuestra que una autenticación exitosa no debe considerarse suficiente evidencia de legitimidad cuando cambia el contexto de sesión.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Cuentas válidas	La identidad cloud comprometida se utiliza para autenticarse en servicios Microsoft.	T1078.004
Persistencia MFA	El actor registra nuevos métodos MFA, dispositivos o OTP para mantener acceso a la identidad.	T1556.006
Descubrimiento	Microsoft Graph se utiliza para enumerar usuarios, identidades y privilegios del tenant.	T1087.004
Datos cloud	El actor busca y descarga contenido alojado en SharePoint y OneDrive.	T1530
Correo	Se recopilan mensajes y adjuntos de los buzones comprometidos mediante APIs.	T1114

Recomendaciones

- Validación de soporte: establecer un canal independiente para verificar llamadas o mensajes que soliciten cambios de MFA, passkeys o SSO.
- Restringir Device Code: bloquear o condicionar el flujo OAuth por código de dispositivo cuando no sea necesario para el negocio.
- MFA resistente al phishing: priorizar autenticadores vinculados a origen y dispositivo, complementados con Conditional Access.
- Monitorear Graph: alertar por enumeración masiva, descargas inusuales y acceso automatizado a SharePoint, OneDrive o Exchange.
- Respuesta: revocar sesiones, retirar métodos MFA añadidos por el atacante y revisar aplicaciones, dispositivos e identidades relacionadas.

ALTA

3.3 [ALTA] GhostCode abusa del flujo OAuth Device Code para obtener tokens después de una autenticación legítima



eSentire publicó el 15 de septiembre de 2026 el análisis de GhostCode, un kit de phishing por código de dispositivo identificado en una campaña iniciada mediante formularios web.

Los actores se presentan como responsables de compras, establecen una conversación legítima y posteriormente envían un enlace de WeTransfer hacia un HTML protegido con contraseña bajo el pretexto de firmar un NDA.

El archivo redirige a una página que muestra un código y solicita a la víctima introducirlo en el portal legítimo de Microsoft.

Cuando el usuario completa el inicio de sesión y el MFA, el atacante recibe tokens asociados al flujo OAuth 2.0 Device Authorization Grant.

eSentire observó posteriormente registro de dispositivos, obtención de tokens de larga duración y recolección de correo.

El uso de páginas reales de Microsoft reduce señales visuales típicas de un formulario de phishing convencional.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Phishing	El actor entrega un archivo HTML mediante un enlace de transferencia dentro de una conversación de negocio.	T1566.002
Ejecución del usuario	La víctima abre el HTML protegido y sigue las instrucciones de autenticación presentadas por el kit.	T1204.002
Robo de tokens	El flujo Device Code permite al atacante obtener tokens OAuth emitidos después de la autenticación de la víctima.	T1528
Registro de dispositivo	Después del acceso, se observaron dispositivos adicionales registrados sobre la cuenta comprometida.	T1098.005
Recolección de correo	La actividad posterior incluyó acceso y recolección de mensajes de correo.	T1114

Recomendaciones

- Device Code: deshabilitar o limitar el flujo OAuth Device Authorization en organizaciones que no requieran este mecanismo.
- Control de HTML: tratar archivos HTML protegidos con contraseña y entregados por servicios de transferencia como contenido de alto riesgo.
- Concientización: advertir que un portal Microsoft legítimo también puede ser utilizado para autorizar una sesión iniciada por un atacante.
- Monitoreo de identidad: alertar por nuevos dispositivos y tokens persistentes inmediatamente después de autenticaciones por código de dispositivo.
- Respuesta: revocar tokens, sesiones y dispositivos registrados, y revisar correo y aplicaciones accedidas tras el evento sospechoso.

4. ADVERSARIOS

CRÍTICA

4.1 [CRÍTICA] BREEZE COMET ataca organizaciones financieras de Brasil para manipular sistemas de pago y realizar transferencias fraudulentas



Google Threat Intelligence Group y Mandiant publicaron el 1 de septiembre de 2026 un análisis de BREEZE COMET, actor con motivación financiera que opera desde 2024 contra servicios financieros, retail y comercio electrónico en Brasil.

Su objetivo es mantener acceso suficiente para interactuar con software bancario, APIs y sistemas de pago como Pix, STR y Boleto, apoyándose en credenciales mTLS y cuentas persistentes cuando logra alcanzarlas.

En compromisos tempranos, Mandiant observó password spraying y llamadas que suplantaban a soporte de TI para convencer a usuarios de instalar AnyDesk.

El grupo también utilizó sitios gubernamentales previamente comprometidos para alojar RMM, infostealers y XWORM, aprovechando la reputación de infraestructura legítima.

Su tooling personalizado automatiza reconocimiento, movimiento lateral, persistencia y exfiltración en múltiples entornos comprometidos.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Fuerza bruta	El actor ha utilizado password spraying para probar credenciales contra organizaciones objetivo.	T1110.003
Acceso remoto	Llamadas de falso soporte inducen a usuarios a instalar herramientas RMM como AnyDesk.	T1219
Transferencia	El actor descarga utilidades y frameworks adicionales desde infraestructura externa o sitios comprometidos.	T1105
PowerShell	Herramientas de reconocimiento fueron observadas ejecutándose en memoria mediante PowerShell.	T1059.001
Cuentas válidas	La operación depende de mantener acceso a cuentas AD o cloud para alcanzar sistemas financieros.	T1078

Recomendaciones

- Vishing y RMM: exigir aprobación formal para instalar herramientas de acceso remoto y verificar por canal independiente toda llamada de soporte.
- Identidades privilegiadas: proteger cuentas con acceso a pagos mediante MFA resistente al phishing, PAM y estaciones administrativas dedicadas.
- Segregar pagos: aislar sistemas Pix, STR y APIs financieras mediante microsegmentación y controles de acceso basados en identidad.
- Protección de mTLS: almacenar claves y certificados en gestores de secretos o HSM con auditoría y rotación controlada.
- Hunting: buscar tooling de BREEZE COMET y correlacionar descargas desde sitios legítimos comprometidos con ejecución de RMM o PowerShell.

CRÍTICA**4.2 [CRÍTICA] storm-2570 mantiene el mismo patrón operativo mientras despliega Qilin, DragonForce, Anubis y BERT**

Microsoft Threat Intelligence publicó el 24 de septiembre de 2026 un análisis de Storm-2570, afiliado de ransomware rastreado desde abril de 2025 y observado en incidentes con Qilin, DragonForce, Anubis y BERT.

Aunque el acceso inicial no está confirmado de forma consistente, el actor repite herramientas y comportamientos post-compromiso: MeshAgent, Atera, ScreenConnect, Splashtop y otros RMM; NetScan y Nmap para descubrimiento; Mimikatz, LaZagne, pypykatz y ntdsutil para credenciales; y PsExec, Impacket, RDP y compartidos administrativos para movimiento lateral.

Antes del impacto, Storm-2570 modifica configuraciones de Microsoft Defender, deshabilita protección en tiempo real y añade exclusiones.

También utiliza Cloudflared o ngrok para túneles y herramientas de transferencia como s5cmd o Rclone para exfiltrar datos antes de desplegar ransomware.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Acceso remoto	El actor utiliza múltiples herramientas RMM comerciales para mantener ejecución interactiva persistente.	T1219
Credenciales AD	ntdsutil se emplea para crear copias de NTDS.dit y material de registro para extracción offline.	T1003.003
Evasión de defensas	Storm-2570 deshabilita protección en tiempo real y modifica exclusiones de Microsoft Defender.	T1562.001
Escritorio remoto	RDP facilita el movimiento lateral y la ejecución interactiva sobre sistemas comprometidos.	T1021.001
Recursos SMB	Los recursos administrativos y compartidos SMB facilitan el movimiento lateral entre sistemas Windows.	T1021.002
Ejecución de servicios	Psexec permite ejecutar comandos de forma remota mediante la creación y ejecución de servicios.	T1569.002
Impacto	La cadena culmina en el despliegue de diferentes familias de ransomware para cifrar sistemas.	T1486

Recomendaciones

- Inventario de RMM: permitir únicamente agentes autorizados y alertar ante MeshAgent, Atera, ScreenConnect o Splashtop no administrados.
- Proteger controladores de dominio: restringir ntdsutil y detectar creación de copias IFM o acceso a NTDS.dit fuera de procedimientos aprobados.
- Tamper protection: impedir cambios no autorizados en Defender, exclusiones antivirus y claves de servicio de seguridad.
- Movimiento lateral: limitar RDP, SMB administrativo y PsExec entre segmentos; aplicar LAPS, PAM y tiering de administración.
- Resiliencia: mantener backups aislados e inmutables y detectar exfiltración hacia almacenamiento cloud antes de la fase de cifrado.

CRÍTICA

4.3 [CRÍTICA] Storm-3168 utiliza service principals comprometidos para reconocimiento y destrucción automatizada de recursos Azure



Microsoft Security Research informó el 25 de septiembre de 2026 sobre Storm-3168, actividad asociada con JADEPUFFER que utilizó service principals comprometidos para operar dentro de Azure.

En un tenant investigado, dos identidades de aplicación fueron usadas con funciones distintas: una para reconocimiento y otra para descubrimiento, recolección de credenciales y acciones destructivas.

Microsoft registró cientos de operaciones de lectura exitosas y observó eliminación de recursos de Azure Storage, Key Vault, Function Apps y App Service, además de intentos sobre Azure SQL.

El actor también apuntó a bloqueos asociados con Site Recovery y Azure Backup, buscando reducir la capacidad de recuperación.

La superposición temporal y la velocidad de las acciones son consistentes con automatización avanzada o comportamiento agentic, aunque la investigación no elimina la participación humana en la operación.

Tácticas, Técnicas y Procedimientos (TTPs) de MITRE ATT&CK

Fase del ataque	Descripción	Referencia MITRE ATT&CK
Explotación	Infraestructura vinculada al actor realizó sondeos sobre rutas sensibles de aplicaciones alojadas en Azure App Service.	T1190
Cuentas cloud	Service principals comprometidos se utilizaron como identidades válidas para operar dentro del tenant.	T1078.004
Descubrimiento cloud	Las identidades enumeraron suscripciones, recursos, máquinas virtuales, Storage y servicios de recuperación.	T1526
Destrucción de datos	Se eliminaron recursos de Storage, Key Vault, Function Apps y App Service; también se intentó afectar Azure SQL.	T1485
Inhibir recuperación	El actor intentó eliminar bloqueos relacionados con Site Recovery y protección de Azure Backup.	T1490

Recomendaciones

- Service principals: rotar secretos y certificados, aplicar privilegio mínimo y eliminar credenciales de aplicación antiguas o no utilizadas.
- Identidades de workload: monitorear autenticaciones, cambios de rol y operaciones ARM inusuales ejecutadas por aplicaciones y automatizaciones.
- Protección de recursos: usar locks, Azure Policy y separación de privilegios para impedir que una sola identidad pueda eliminar producción y backups.
- Detección de destrucción: alertar por ráfagas de operaciones DELETE sobre Storage, Key Vault, App Service, Recovery Services y bases de datos.
- Respuesta cloud: ante compromiso de una identidad de aplicación, revocar credenciales, revisar permisos heredados y reconstruir la secuencia completa de API calls.

5. INDICADORES DE COMPROMISO

5.1 Direcciones IP

104[.]37[.]188[.]94	98[.]142[.]252[.]140	185[.]157[.]160[.]251
154[.]127[.]53[.]78	72[.]167[.]48[.]63	45[.]131[.]66[.]106
193[.]23[.]118[.]155	209[.]99[.]188[.]28	34[.]153[.]223[.]102
208[.]64[.]33[.]90	209[.]141[.]43[.]95	64[.]20[.]53[.]230
208[.]94[.]246[.]53	99[.]84[.]67[.]186	

5.2 Dominios

deadhub[.]org	secure-passkey[.]com
gexwalltool[.]com	setupmypasskey[.]com
x-wolverine[.]servebbs[.]com	integratedsso[.]com
advancedplacyncement[.]vu	oktasession[.]com
certifiycationedge[.]vu	windwsecurity[.]run
digitaltrafwrrficsystems[.]vu	ntp.timesysnc[.]net
passkeyhelpdesk[.]com	time.microsoft[.]run

5.3 Hashes

c513a7346484ee69a2931c4a89956ee50aa63e4366ef989315e669d8f10d7485
8c3b41ea5a85778145a6e5772bfee2eb0f8b027d0af199fb71a76dfb8bb29e5a
6bb4372d0d02ec87b76409f69d445a93910964f8db457bafab97a011da59e73
40d253480f752805e58c21266e40afe99afc96fee0d355732af5bea459db1dd
bf92a287a3d79afb73a3f2d38877ec37c22a9f4a7d6ac2e0385472298f384fc8
3b22605244dbace8f0c07c2c599f88c4b831bb07e9998b869a5da2759d27ceec
2214907e696bad85bde1d90c943ef66e413d7a5c6d7596ced25b74441200439a
c0db6ddd6222d02ad7490399d33c61ded0076f0037409dc8498924458646d78a
6d4012e0dd3b56a3e52857734fa0d582cdf3c56f0e5decc8005c882d1d1c6ceb
f139b4ca15feffb7a6633ec1a431c5c604b397576b56b5c863ae8fe4fa14db4f
48d3ecbb9e0b6babe6e53e2082a076bad07ef61ccd98dcc8b9e4f390b937788b
37fcbcb21d16866784050682c58424c91d3a736f6fd599271fa6e53cf5ca8a92

6. FUENTES

- 6.1 <https://www.huntress.com/blog/exodus-crypto-wallet-installer-rat>
- 6.2 <https://www.elastic.co/security-labs/threat-command/revstealer-credential-harvesting-infostealer>
- 6.3 <https://securelist.com/moviereaper-malware-torrent-odyssey-solana/121344/>
- 6.4 <https://www.fortinet.com/jp/blog/threat-research/uncovering-a-sectopratt-variant-embedded-in-legitimate-software>
- 6.5 <https://helpx.adobe.com/security/products/magento/apsb26-146.html>
- 6.6 <https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-n9k-s1-rce-EH8dEtr.html>
- 6.7 <https://status.n-able.com/2026/09/06/n-central-2026-3-hotfix-4-cve-2026-86218/>
- 6.8 <https://www.jpccert.or.jp/at/2026/at260028.html>
- 6.9 <https://www.huntress.com/blog/inside-knight-office-m365-aitm-attack>
- 6.10 <https://www.microsoft.com/en-us/security/blog/2026/09/09/passkey-themed-social-engineering-leads-identity-cloud-compromise/>
- 6.11 <https://www.esentire.com/blog/ghostcode-dissecting-a-novel-device-code-phishing-kit>
- 6.12 <https://cloud.google.com/blog/topics/threat-intelligence/financially-motivated-threat-actor-breeze-comet-targets-brazil>
- 6.13 <https://www.microsoft.com/en-us/security/blog/2026/09/24/beyond-ransomware-tracking-storm-2570-consistent-tradecraft-across-deployments/>
- 6.14 <https://www.microsoft.com/en-us/security/blog/2026/09/25/storm-3168-agentic-driven-cloud-attacks-using-compromised-service-principals/>